IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	No. 1:15-CR-124
	)	
v.	)	The Honorable T.S. Ellis, III
	)	
MUNEEB AKHTER,	)	Hearing: July 7, 2017
	)	
Defendant.	)	

POSITION OF THE UNITED STATES WITH RESPECT TO DEFENDANT'S SUPERVISED RELEASE VIOLATIONS

The United States of America, pursuant to 18 U.S.C. § 3583 and Rule 32.1 of the Federal Rules of Criminal Procedure, by and through Dana J. Boente, United States Attorney, Colleen E. García, Assistant United States Attorney, and Kellen S. Dwyer, Assistant United States Attorney, submits the following memorandum on the supervised release violations of Muneeb AKHTER ("the defendant"). The defendant has repeatedly violated the terms of his release, and openly defied his probation officer and the Bureau of Prisons (BOP). Given the defendant's repeated and flagrant violations, along with his demonstrated lack of remorse, the United States recommends that the Court revoke the defendant's supervised release and impose the statutory maximum of two years of imprisonment.

I. Background

In 2014 and 2015, AKHTER secretly installed computer code on a victim company's computer ("the Underlying Company") that would allow him and his co-conspirators to steal information, including compromised credit cards, along with the names, addresses, phone numbers, and email addresses of the victims. Presentence Investigation Report (PSR) at ¶¶ 39 &

42-45. AKHTER accessed the computer remotely, using his personal laptop. AKHTER and his co-conspirators then made purchases via the Internet on multiple vendors' websites, using the stolen information.[1] PSR at ¶ 17. He and his brother also conspired, and attempted, to hack into computers at the United States Department of State for the purpose of accessing and unilaterally approving visa applications for payment, and creating passports and visas for sale on the dark net. PSR at ¶ 77.

The defendant was initially arrested on a criminal complaint charging credit card fraud on February 27, 2015. Dkt. No. 7. He was placed on pretrial supervision on March 2, 2017. *Id.* & Dkt. No. 13. While on release, he violated the terms of his supervision by contacting his co-defendant brother about the case and by obstructing justice when he sought to, and did, isolate his co-conspirator from the law enforcement officers investigating them. Dkt. No. 31. The defendant paid for his co-conspirator's travel overseas and encouraged him to remain a fugitive. *Id.* The defendant also boasted to his co-conspirator that he had obtained the passport information of one of the lead law enforcement officers on his case, which the defendant said could be valuable to criminals. *Id.* AKHTER's bond was revoked on May 8, 2015. Dkt. No. 34.

On June 26, 2015, AKHTER pleaded guilty to six counts of a Criminal Indictment charging him with: Count One—conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1343 and 1349; Count Two—conspiracy to access a protected computer without authorization, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i)-(iii) and 371; Count Seven—access of a protected computer without authorization, in violation of

[1] When contacted by a Washington Post reporter in July 2014 regarding a search warrant for his residence, AKHTER deleted information from his computer and cell phone. Dkt. No. at ¶ 14; PSR at 46.

Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i), (iii); Count Eight—conspiracy to access a government computer without authorization, in violation of Title 18, United States Code, Sections 1030(a)(2)(B) and (c)(2)(B)(i)-(iii) and 371; Count Ten—making a false statement in violation of Title 18, United States Code, Section 1001(a)(2); and Count Twelve—obstruction of the due administration of justice, in violation of Title 18, United States Code, Sections 1503 and 3147(1). Dkt. Nos. 48–49.

In late July 2015, while awaiting sentencing, the defendant used stolen login credentials to access a restricted area within the Detention Center's law library computer network. At that time, he surreptitiously, and without authorization, created a system that allowed inmates to send private messages to each other. Dkt. No. 31.

On October 2, 2015, the defendant was sentenced to 39 months in prison and three years of supervised release. Dkt. Nos. 77 & 83.[2] His sentence was later reduced to 21 months in prison. Dkt. No. 94. AKHTER began his prison sentence on October 26, 2015, after serving continuous time in BOP custody since May 8, 2015, and he was released from prison on December 27, 2016. Prior to his release, AKHTER was sanctioned for having contraband on his person, to wit cell phones.[3]

Following his release, AKHTER was placed on supervised release until December 27, 2019. The standard conditions of his release prohibited him from committing any additional crimes. The special conditions of release required the installation of computer monitoring software on any computer to which he had access. Senior U.S. Probation Officer Bethany Erding also

[2] At the time of sentencing, AKHTER's guidelines range was 57 to 71 months. PSR at ¶ 197.
[3] According to BOP records, the sanction date was January 21, 2016.

instructed AKHTER to notify her of all computers and smart phones he used, to refrain from using additional operating systems without her knowledge, and to report all email addresses he used.

II. Violations Currently Before the Court

On May 17, 2017, the U.S. Probation Office and the U.S. Attorney's Office, Eastern District of Virginia, were notified by the owner of Victim Company 1 that AKHTER was "still scamming people." After speaking with the owner, Senior Probation Officer Bethany Erding learned from the owner that AKHTER registered for a training class provided by Victim Company 1. However, the class fee was charged to a PayPal account in the name of M.K. on Still Meadow Lane in West Bloomfield, MI. AKHTER attended the training from April 7, 2017 to April 8, 2017 and received a certification. Later, Victim Company 1 was notified by PayPal that M.K. had filed a complaint with PayPal, and that PayPal would not be paying the $1300 class fee to Victim Company 1. Therefore, Victim Company 1 suffered a loss of $1300.

Upon further review of the RemoteCOM computer monitoring software, the U.S. Probation Office has seen Order Confirmation Emails sent to email addresses controlled by AKHTER and accessed while under computer monitoring:

a. Amazon purchase confirmations have been emailed to email addresses accessed by AKHTER, including munibee@hotmail.com. Screen captures of the Amazon purchases showed that the items included comic books shipped to AKHTER's brother, Sohaib Akhter, at the Federal Correctional Institution in Ashland, Kentucky. The Amazon purchases were made in the name of K.M. on Brickell Ave. in Miami, FL.

b. A SAKS purchase confirmation had been emailed to email addresses accessed by AKHTER. The SAKS purchase was made in the name of C.B. on Breton Court in Reston, VA.

After additional review of the computer monitoring software, Officer Erding saw that there was a nine-day gap in the computer monitoring, during which time there were no keystrokes made or websites accessed. According to RemoteCOM, which administers the computer monitoring program, if the computer is on, the monitoring will report every keystroke made and website accessed. A nine-day gap in monitoring would ordinarily indicate that the monitored computer was off during that time. However, Order Confirmation emails sent to emails controlled and accessed by AKHTER show Amazon purchases were made during the nine-day gap in monitoring. For AKHTER to engage in online activity that was not captured by the computer monitoring software, he would have had to access an unmonitored device and/or access a virtual operating system that was not being monitored. In her discussions with REMOTECom, Officer Erding learned that AKHTER was using a virtual monitoring system.

Then, on June 2, 2017, Officer Erding conducted a surprise home inspection at AKHTER's residence. She saw multiple external hard drives and thumb drives in AKHTER's bedroom, which were contraband under the terms of his supervised release. Officer Erding also found a box of cell phones, including smart phones, in what used to be his mother's bedroom.[4] Because AKHTER had been prohibited from keeping these phones, AKHTER's mother had previously told Officer Erding that she (his mother) would retain the box of cell phones in her possession. However, the box of cell phones was left in the home when AKHTER's mother moved to Texas. Under his

[4] AKHTER had previously been living with his mom, dad, sister, and grandmother following his release. However, his mom, dad, and sister have since moved to Texas.

conditions of release, AKHTER is not allowed to have access to these phones because they are unmonitored.

In addition, Officer Erding saw a desktop computer in AKHTER's residence that had not been reported to her. AKHTER told Officer Erding that the computer belonged to his grandmother. All computers in AKHTER's home that do not belong to AKHTER are required to be password protected, and AKHTER is not allowed to have the password. However, Officer Erding was able to access the computer without a password. The desktop computer supposedly belonging to the grandmother does not have computer monitoring software installed.

On June 8, 2017, Officer Erding filed a petition charging that the defendant violated the terms of his supervised release by failing to comply with the requirements of his computer monitoring program, failing to be truthful with his probation officer, failing to report as directed to his probation officer, failing to report his employment to his probation officer, and failing to abide by federal laws. Dkt. Nos. 113 & 115.

On June 9, 2017, agents of the FBI executed federal search warrants (Case Nos. 1:17-SW-309 and 1:17-SW-311) at the premises located at 7510 Chancellor Way, Springfield, VA 22153. Agents seized over 30 items during the execution of the search warrant to include an Automated Teller Machine (ATM) keypad, an MSR X6 card reader, a smart card reader SDX, and an MSR605 card reader. These devices allow a user to read data on or write data to a card, such as a credit card or Common Access Card (CAC) used to manage security to facilities. Agents did observe credit cards in the house and in AKHTER's wallet in the house; however, these cards were not seized at the time and were and left in the house. Also, during the execution of that search, FedEx delivered a laptop-sized box with with FedEx Tracking Number 7375 8382 2610 and Dell Order Number 226170172. The shipment was addressed to "MICROSOFT, JAMES KIRCHER, 7510 Chancellor

Way, Springfield, VA 22153." The Agents did not seize the FedEx package at the time.

Later that day, on June 9, 2017, the defendant contacted his co-conspirator from the underlying case to check his wallet in his house to make sure his access card was still there. This contact was a violation of his terms of supervised release. Dkt. No. 124.

On June 12, 2017, FBI agents confirmed by speaking to the victims K.M. and M.K. that they were customers of the Underlying Company. On June 15, FBI agents confirmed that C.B. was also a customer of the same victim company from the underlying crime. Therefore, AKHTER continues to use customer information from the Underlying Company to purchase items for himself and others. On June 16, 2017, FBI agents obtained the consent of the owner of the Underlying Company to image the business computers and review customer records for potential additional victims.

On June 22, 2017, agents of the FBI executed a second federal search warrant (Case No. 1:17-SW-334) at the premises located at 7510 Chancellor Way, Springfield, VA 22153. At that time, the agents seized the box and the cards mentioned above. Some cards were embossed with the defendant's name, at least one card was embossed with his co-defendant brother's name, and some cards had not yet been embossed. Upon further examination of the cards seized, FBI agents discovered that the cards are encoded with the financial information of C.B. and additional victims.

On June 23, 2017, Cellebrite imaging of the cell phones recovered from Akhter's residence during the lawful search on June 9 revealed four associated email accounts—amkircher724@gmail.com, hackinback@gmail.com, meemical@gmail.com, muneeb@muneebakhter.com—and one account that is or is associated with nsalookup@gmail.com. The first email account belongs to victim A.K. The email account meemical@gmail.com contains emails related to purchases from the following vendors and

victims: AMC tickets (in the name of victim C.G.), B&H (in the name of victim V.S.), and Seamless from Granada restaurant (in the name of victim T.W.). Content from the emails associated with nsalookup@gmail.com contain fields and values from the website checkout of the Underlying Company, including payment information.

Review of the customer records of the Underlying Company reveal the following transactions by the victims mentioned above:

a. Victim A.K. placed 4 orders from underlying victim company in June 2017.

b. Victim C.G. placed 10 orders between January 2016 and May 2017.

c. Victim V.S. placed 10 orders between May 2015 and May 2017.

d. Victim T.W. placed 5 orders between October 2015 and May 2017.

e. Victim C.B. placed 7 orders between April 2016 and May 2017.

f. Victim K.M. placed 7 orders between September 2013 and April 2017.

g. Victim M.K. placed 7 orders between March 2015 and March 2017.

This further demonstrates that AKHTER continues to use customer information from the Underlying Company to purchase items for himself and others.

Then, on June 23, 2017, the U.S. Probation Office and the U.S. Attorney's Office were notified that the defendant had committed violations while in the custody of the Bureau of Prisons, namely, that he had established a intranet system on the computers that the inmates could use to privately message each other. This is the same violation he committed while awaiting sentencing for the underlying crime in 2015, after his bond had been revoked. Dkt. No. 124.

III. Legal Standard

Supervised release revocation hearings are not formal trials. *See United States v. Woodrup*, 86 F.3d 359, 361-62 (4th Cir. 1996). A court need only find by a preponderance

of the evidence that the defendant violated a condition of supervised release to support a revocation order. *See* 18 U.S.C. § 3583(e)(3); *see also United States v. Copley*, 978 F.2d 829, 831 (4th Cir.1992). Upon finding that a defendant has violated a condition of supervised release, a court may (i) revoke supervised release and impose a term of imprisonment authorized by statute; (ii) under certain conditions, extend the term of supervised release; or (iii) modify, reduce, or enlarge the conditions of supervised release. *See* 18 U.S.C. § 3583(e).

In considering what action to take upon a violation of supervised release, Section 3583(e) directs courts to consider certain factors set forth in Section 3553(a). Specifically, courts are to consider, to the extent applicable: (i) the nature and circumstances of the offense, and the history and characteristics of the defendant; (ii) the need for adequate deterrence; (iii) the need to protect the public from further crimes of the defendant; (iv) the need to provide the defendant with training or treatment; (v) applicable guidelines issued by the Sentencing Commission; (vi) pertinent policy statements issued by the Sentencing Commission; (vii) the need to avoid unwarranted sentencing disparities; and (viii) the need to provide restitution to victims. *See* 18 U.S.C. §§ 3553(a), 3583(e).

IV. Analysis

The Guidelines provide non-binding policy statements with respect to supervised release violations. *See* U.S.S.G. § 7Al; *see also United States v. Davis*, 53 F.3d 638, 640 (4th Cir. 1995). The Guidelines also present recommended incarceration ranges upon revocation based upon the defendant's criminal history category and the grade of the violation. *See* U.S.S.G. § 7B1.4. Where the defendant commits multiple violations, the defendant's Guidelines range is determined by the violation having the most serious grade. *Id.* § 7B1.1(b).

Here, the defendant's new crimes qualify as Grade A violations. Under the Guidelines,

any "federal, state, local offense punishable by a term of imprisonment exceeding twenty years" is a Grade A violation. *Id.* § 7B1.1(a)(1). The new crimes committed are, at minimum, Wire Fraud, in violation of 18 U.S.C. § 1343 (thirty-year maximum), and Access Device Fraud, in violation of 18 U.S.C. §§ 1029(a)(2) and (a)(5) (ten-year and fifteen-year maximums respectively). Thus, the defendant's new crimes constitute a Grade A violation of the terms of his supervised release, for which revocation is mandatory. *See* U.S.S.G. § 7B1.3(a)(1).

At the time of the defendant's underlying convictions in 2015, he had a Category I Criminal History. For a Grade A violation committed by a defendant with a Category I Criminal History, the Guidelines recommend 12 to 18 months' imprisonment. *See id.* § 7B1.4(a). However, Application Note 4 of section 7B1.4(a) states, "Where the original sentence was the result of a downward departure (*e.g.*, as a reward for substantial assistance), or a charge reduction that resulted in a sentence below the guideline range applicable to the defendant's underlying conduct, an upward departure may be warranted." *Id.* at Application Note 4. Because the defendant's underlying conviction were Class C and D felonies, the statutory maximum prison sentence upon revocation is two years. *See* 18 U.S.C. § 3583(e)(3).

The Court may also impose an additional term of supervised release after imprisonment, not to exceed the term of supervised release authorized by statute for the original offense, less any term of imprisonment imposed upon revocation. *See* 18 U.S.C. § 3583(h). Here, the maximum term of supervised released authorized for the defendant's original offenses is three years. *See* 18 U.S.C. § 3583(b)(2).

V. Recommendation

The Government respectfully recommends that the Court revoke the defendant's supervised release and sentence him to the statutory maximum of two years of imprisonment, an

upward departure from the applicable Guidelines range of 12 to 18 months. The defendant has repeatedly violated the conditions of his release, and has openly defied his probation officer and the Bureau of Prisons (BOP). In addition, his re-victimization of the Underlying Company and his commission of the same offenses as before, both while on release and while detained, demonstrate a concerning lack of remorse.

Given the defendant's repeated and flagrant violations, along with his demonstrated lack of remorse, a statutory maximum sentence of two years is necessary to promote respect for the law and to protect the public from further crimes by the defendant. It would also provide an opportunity for correctional treatment. Such a sentence would be sufficient, but not greater than necessary, to satisfy the factors set forth in 18 U.S.C. § 3553(a). The Government also respectfully requests that the defendant's imprisonment be followed by a term of supervised release, and defers to the Court as to the length of that term.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: /s/
Colleen E. García
Kellen S. Dwyer
Assistant United States Attorney
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314

CERTIFICATE OF SERVICE

I hereby certify that on July 5, 2017, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic copy to the following:

Nader Hasan, Esq.
10603 Judicial Dr.
Fairfax, VA 22030
Office: 703-865-5590
Fax: 703-865-5597
Nhasan@NaderHasan.com

In addition, I hereby certify that on July 5, 2017, I emailed a copy of the foregoing to

Bethany Erding
U.S. Probation Officer
Bethany_Erding@vaep.uscourts.gov

Respectfully submitted,

Dana J. Boente
United States Attorney

By: /s/

Colleen E. García
Kellen S. Dwyer
Assistant United States Attorneys
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: (703) 299-3700
Fax: (703) 299-3980
Email: Colleen.E.Garcia@usdoj.gov